APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/016,558	12/06/2001	Albert Young	3730.US.P	6325

56436   7590   07/26/2007
3COM CORPORATION
350 CAMPUS DRIVE
MARLBOROUGH, MA 01752-3064

EXAMINER
SIMITOSKI, MICHAEL J

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
07/26/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _08 May 2007_.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _61-73_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _61-64,68,69 and 73_ is/are rejected.

7)☒ Claim(s) _65-67 and 70-72_ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _14 February 2002_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   The response of 5/8/2007 was received and considered.

2.   Claims 61-73 are pending.

Response to Arguments

3.   Applicant has canceled the previously examined claims 1-60. New grounds of rejection

are presented herein.

Claim Objections

4.   Claims 62 & 73 are objected to because of the following informalities:

a.   Regarding claim 62, the claim is believed to depend from claim 61.

b.   Regarding claim 73, the claim should be directed to the computer-useable

medium of claim 69.

Appropriate correction is required.

Claim Rejections - 35 USC § 112

5.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the
> subject matter which the applicant regards as his invention.

6.   Claims 61-62, 68 & 73 are rejected under 35 U.S.C. 112, second paragraph, as being

indefinite for failing to particularly point out and distinctly claim the subject matter which

applicant regards as the invention.

c.   Regarding claim 61, the claim recites "authenticating ... using the key and

Extensible Authentication Protocol-Transport Layer Security" (lines 6-8); however, the

metes and bounds of "Extensible Authentication Protocol-Transport Layer Security" is

unclear because this describes, as best understood, the security provided by a protocol.

For the purposes of this Office Action, this limitation is understood to mean that the EAP-

TLS protocol is employed.

d.   Regarding claims 68 & 73, the scope of the limitations "user_name" and

"user_credentials" is unclear as the limitations are written in the form of a data

structure (i.e. it is unclear if these limitations are meant to include further limitations or

are merely names). *For the purpose of this Office Action, the above limitations are*

considered to be names.

e.   Any claims rejected under 35 U.S.C. §112, but not specifically addressed, is

rejected based on its depending from a claim rejected under the same section. Further,

all claims addressed below regarding 35 U.S.C. §§102-103 are addressed as best

understood.

Claim Rejections - 35 USC § 103

7.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness

rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art
> are such that the subject matter as a whole would have been obvious at the time the invention was made to a
> person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be
> negatived by the manner in which the invention was made.

8.   Claims 61-64 & 69 are rejected under 35 U.S.C. 103(a) as being unpatentable over "PPP

EAP TLS Authentication Protocol" by Aboba et al. (**Aboba**) in view of U.S. Patent 7,039,190 to

Engwer et al. (**Engwer**) and "Remote Authentication Dial In User Service (RADIUS)" by Rigney et

al. (**Rigney**).

Regarding claims 61-62, Aboba discloses mutually authenticating a client device (peer, p.

4, ¶4, EAP server verifies peer's digital signature) and a server (authenticator, p. 5, ¶2, peer

verifies EAP server's authentication response) using message digests (signed responses, p. 3, ¶6

& p. 4, ¶4) to perform a shared key exchange (shared master secret exchange, p. 4, ¶4) to

produce an authenticated client device (peer) and a key (master secret, p. 4, ¶4 & p. 21, ¶1).

Aboba lacks the server being an access point, lacks a wireless connection and lacks

authenticating, via the access point, a user of the authenticated client device (peer) to an

authentication server using the key and Extensible Authentication Protocol-Transport Layer

Security. However, Engwer teaches a data confidentiality algorithm is used between a mobile

unit of a wireless LAN and an access point (col. 1, lines 32-34) where the mobile unit is

authenticated to the access point to discourage an interloper from eavesdropping on

communications between an access point and a mobile unit (col. 1, lines 32-34). Therefore, it

would have been obvious to one having ordinary skill in the art at the time the invention was

made to modify Aboba such that the peer is a mobile unit and the authenticator is an access

point communicating via a wireless connection. One of ordinary skill in the art would have

been motivated to perform such a modification to use the EAP-TLS protocol in a mobile

environment to provide confidentiality, as taught by Engwer (col. 1, lines 32-34). As modified,

Aboba lacks the step of authenticating the user. However, Rigney teaches authenticating a user

(RADIUS request containing user's password, p. 5, §2) to a central authentication server (radius

server) (p. 5, §2, ¶3) using PPP (p. 5, §2, ¶1) for the purpose of authenticating users and

delivering services based on that authentication (p. 3, §1, ¶2). Therefore, it would have been

obvious to one having ordinary skill in the art at the time the invention was made to modify

Aboba's EAP TLS protocol (as modified by Engwer) to authenticate a user to a RADIUS server

using the key generated and using the authenticated client device (Aboba's peer). One of

ordinary skill in the art would have been motivated to perform such a modification to

authenticate the user securely and deliver services to the user, as taught by Rigney (p. 3, §1, ¶2

& p. 5, §2).

Regarding claims 63-64 (and by similar rationale, claim 69), Aboba discloses first

authenticating a server (authenticator) to an unauthenticated client device (peer, EAP server

sends authentication response, p. 3, ¶6) and second authenticating the unauthenticated client

device (peer) to the server (peer's signed authentication response, p. 4, ¶4) to produce an

authenticated client device (peer) and a key (p. 4, ¶4 & p. 21, ¶1). Aboba lacks the server being

an access point, lacks a wireless connection and lacks authenticating, via the access point, a

user of the authenticated client device (peer) to a central authentication server using the key.

However, Engwer teaches a data confidentiality algorithm is used between a mobile unit of a

wireless LAN and an access point (col. 1, lines 32-34) where the mobile unit is authenticated to

the access point to discourage an interloper from eavesdropping on communications between

an access point and a mobile unit (col. 1, lines 32-34). Therefore, it would have been obvious to

one having ordinary skill in the art at the time the invention was made to modify Aboba such

that the peer is a mobile unit and the authenticator is an access point communicating via a

wireless connection. One of ordinary skill in the art would have been motivated to perform

such a modification to use the EAP-TLS protocol in a mobile environment to provide

confidentiality, as taught by Engwer (col. 1, lines 32-34). As modified, Aboba lacks the step of

authenticating the user. However, Rigney teaches authenticating a user (RADIUS request

containing user's password, p. 5, §2) to a central authentication server (radius server) (p. 5, §2,

¶3) using PPP (p. 5, §2, ¶1) for the purpose of authenticating users and delivering services

based on that authentication (p. 3, §1, ¶2). Therefore, it would have been obvious to one

having ordinary skill in the art at the time the invention was made to modify Aboba's EAP TLS

protocol (as modified by Engwer) to authenticate a user to a RADIUS server using the key

generated and using the authenticated client device (Aboba's peer). One of ordinary skill in the

art would have been motivated to perform such a modification to authenticate the user

securely and deliver services to the user, as taught by Rigney (p. 3, §1, ¶2 & p. 5, §2).

9.   Claims 68 & 73 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Aboba**,

Engwer and **Rigney**, as applied to claims 63 & 69 above.

Regarding claims 68 & 73, Aboba, as modified, teaches the invention described above,

but lacks the steps claimed in claim 68. However, Rigney teaches a method in one form of the

RADIUS protocol called challenge/response, comprising receiving at a client device (client), a

request originating from a central authentication server (RADIUS server) for a user_name and

user_credentials (challenge is given from RADIUS server to client asking for a response, p. 7,

¶4, the response containing a User-name and user-password), transmitting said user_name and

said user_credentials to said central authentication server (RADIUS server, p. 7, ¶4) and

employing said user_name and said user_credentials at said central authentication server

(RADIUS server, accept or reject, p. 7, ¶4). Therefore, it would have been obvious to one having

ordinary skill in the art at the time the invention was made to modify Aboba, as modified

above, to further include the challenge response authentication method of authenticating the

user (and hence use the access point as the proxy for the messages described in Rigney). One

of ordinary skill in the art would have been motivated to perform such a modification to require

that the user require a device to authenticate, as taught by Rigney (p. 7, ¶1).

Allowable Subject Matter

10.   Claims 65 & 70 are objected to as being dependent upon a rejected base claim, but

would be allowable if rewritten in independent form including all of the limitations of the base

claim and any intervening claims.

   f.   Regarding claims 65 & 70 (and by dependence, claims 66-67 & 71-72), the prior

   art of record fails to teach or disclose, either alone or in combination, a digest including

   a one-way hash function operating on said first random number, said device identifier

   and a first secret shared between said wireless access point and said unauthenticated

   client device, determining a second digest comprising a one-way hash function

   operating on said first random number, said device identifier and said first secret and

comparing said first and second digests at said unauthenticated client device, in

combination with the remaining elements of the claims.

.

Conclusion

11.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure.

g.   The Halasz reference is cited for teaching EAP-GSS between a client and access

point (p. 5, slide 1) and then EAP-GSS over RADIUS with an authentication server (p. 5,

slide 1).

12.   Applicant's amendment necessitated the new ground(s) of rejection presented in this

Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is

reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS

from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of

the mailing date of this final action and the advisory action is not mailed until after the end of

the THREE-MONTH shortened statutory period, then the shortened statutory period will expire

on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a)

will be calculated from the mailing date of the advisory action. In no event, however, will the

statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the
examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-
3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's
supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the
organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent
Application Information Retrieval (PAIR) system. Status information for published applications
may be obtained from either Private PAIR or Public PAIR. Status information for unpublished
applications is available through Private PAIR only. For more information about the PAIR
system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private
PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you
would like assistance from a USPTO Customer Service Representative or access to the
automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJS

July 16, 2007

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100